PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-301489
(43)Date of publication of application : 13.11.1998

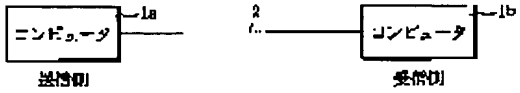
(51)Int.Cl. G09C 1/00
H04K 1/06
H04L 9/06

(21)Application number : 09-104634
(22)Date of filing : 22.04.1997

(71)Applicant : TAISEI CORP
(72)Inventor : NOMURA KIYOUSUKE

(54) DATA CONVERTER

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce the cost, time and labour required to develop the ciphering/ deciphering software compact in size by dividing the prescribed area of data so that plural area having a prescribed length are constituted and a pair of areas, which are combined employing a specific rule, and a similar pair of areas are exchanged.
SOLUTION: This converter is constituted of a computer 1a which ciphers plain data and transmits the data and a computer 1b which deciphers the received ciphered data. The computer 1a and 1b are connected by a data transmitting path 2. In the converter, plain data are divided into the areas having a prescribed length for the ciphering. Then, the divided areas are made into pairs with other areas by a specific combination and these areas are exchanged. On the other hand, during a deciphering, the ciphered data are divided into the areas having a prescribed length. Then, each area is made into a pair with another area employing the same combination used during the ciphering and these areas are exchanged.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－301489

(43)公開日　平成10年(1998)11月13日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ａ
Ｈ０４Ｋ	1/06		Ｈ０４Ｋ	1/06	
Ｈ０４Ｌ	9/06		Ｈ０４Ｌ	9/00	６１１Ｚ

審査請求　未請求　請求項の数７　ＯＬ　（全 12 頁）

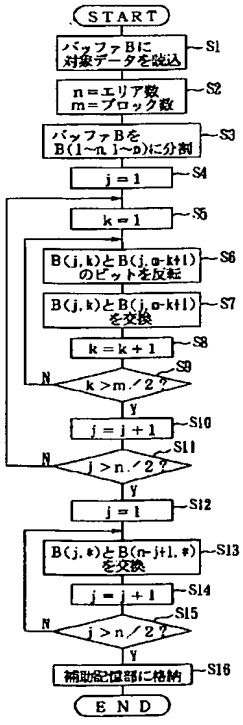
(21)出願番号　特願平9－104634

(22)出願日　平成９年(1997)４月22日

(71)出願人　000206211
大成建設株式会社
東京都新宿区西新宿一丁目25番１号
(72)発明者　野村　享右
東京都新宿区西新宿一丁目25番１号　大成建設株式会社内
(74)代理人　弁理士　森　哲也　（外３名）

(54)【発明の名称】　データ変換装置

(57)【要約】
【課題】　暗号化／復号化ソフトを開発するために要する費用や時間、または手間などを大幅に削減するとともに、コンパクトなサイズの暗号化／復号化ソフトを開発することができるデータ変換装置を提供する。
【解決手段】　コンピュータの記憶手段に格納されているデータを、暗号化および復号化するデータ変換装置において、データの所定領域を所定長のエリアが複数個構成されるように分割するデータ分割手段と、特定の組み合わせで対にしたエリア同士を交換するエリア交換手段と、を備える。



【特許請求の範囲】

【請求項１】　コンピュータの記憶手段に格納されているデータを、暗号化及び復号化するデータ変換装置において、

データの所定領域を所定長のエリアが複数個構成されるように分割するデータ分割手段と、特定の組み合わせで対にした前記エリア同士を交換するエリア交換手段と、を備えることを特徴とするデータ変換装置。

【請求項２】　前記データ分割手段は、前記所定領域を前記エリアが偶数個構成されるように分割することを特徴とする請求項１記載のデータ変換装置。

【請求項３】　前記エリア交換手段は、前記すべてのエリアを必ず一度だけ交換する単位交換処理を、少なくとも１回実行することを特徴とする請求項２記載のデータ変換装置。

【請求項４】　前記データ分割手段は、さらに前記エリアを所定長のブロックが複数個構成されるように分割するブロック分割処理を、前記すべてのエリアについて等しく実行し、前記エリア交換手段は、同一エリア内で特定の組み合わせで対にした前記ブロック同士を交換するブロック交換処理を、前記すべてのエリアについて等しく実行することを特徴とする請求項１、２又は３記載のデータ変換装置。

【請求項５】　前記データ分割手段は、前記エリアを前記ブロックが偶数個構成されるように分割することを特徴とする請求項４記載のデータ変換装置。

【請求項６】　データの前記所定領域を構成するビットを反転するビット反転手段を備えることを特徴とする請求項１、２、３、４又は５記載のデータ変換装置。

【請求項７】　前記エリアを対にする組み合わせを特定するための特定キーを入力する特定キー入力手段を備え、

前記エリア交換手段は、特定キー入力手段から入力された特定キーに基づいて前記各エリアを対にすることを特徴とする請求項１、２又は６記載のデータ変換装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術の分野】本発明は、データを暗号化および復号化するデータ変換装置に係り、特に、暗号化データを生成するときと同一の処理で、その暗号化データを復号化することのできるデータ変換装置に関する。

【０００２】

【従来の技術】従来のデータ変換装置としては、通信データの盗聴、改ざんなどの不正アクセスから通信データを保護するために用いられる暗号化技術がある。これには、例えば、ソフトウェアを利用してデータを暗号化および復号化するものがあり、次のようにしてデータの送受信を行う。

【０００３】送信元コンピュータでは、データを送信しようとする送信者が暗号化ソフトを利用し、送信対象となる平文データを、送信者によって指定された所定の暗号キーに基づいて暗号化し、その暗号化データを送信する。

【０００４】このとき、例えば、ＤＥＳ(Data Encryption Standard)方式によってデータを暗号化する暗号化ソフトは、図８（ａ）に示すように、平文データを暗号化するデータ処理部と、指定された暗号キーから暗号化するために必要なキー情報系列を生成するキースケジューラ部とで構成されている。データ処理部では、６４ビットごとに平文データを分割し、分割したデータ列をキースケジューラ部で生成されたキー情報系列を用い、同一の変換を１６段繰り返して６４ビットの暗号化データを生成する。一方、キースケジューラ部では、６４ビットで構成される暗号キーを用いて１６段のキー情報系列K_1、K_2、…、K_{16}を生成する。なお、図中、ｆは、図８（ｂ）に示すように、非線形変換であって、６ビット入力４ビット出力のテーブルで与えられる８個のＳボックスからなっている。

【０００５】一方、送信先コンピュータでは、データを受信した受信者が復号化ソフトを利用し、受信した暗号化データを、受信者によって指定された所定の復号キーに基づいて復号化する。

【０００６】このとき、例えば、ＤＥＳ方式によってデータを復号化する復号化ソフトは、図８（ａ）において、キースケジューラ部で生成するキー情報系列を暗号化したときとは逆に、K_{16}、K_{15}、…、K_1 とすれば、元の平文データが得られる。ただし、受信者が指定した復号キーと送信者が指定した暗号キーとが一致しなければ、元の平文データを得ることができない。

【０００７】

【発明が解決しようとする課題】しかしながら、従来のデータ変換装置は、暗号化するときのキー情報系列に対して、復号化するときのキー情報系列を逆の順序で生成する必要があるため、暗号化するためのデータ処理部と復号化するためのデータ処理部とを個別に設計しなければならなかった。

【０００８】このため、従来、暗号化／復号化ソフトを開発する際には、暗号化または復号化するためのデータ処理部をそれぞれ個別に設計する必要があること、また、暗号化データ処理部で生成された暗号化データを、復号化データ処理部で確実に復号化することができるか否かを厳密にテストする必要があることなどから、費用や時間や手間などがかかるとともに、完成するソフトのデータ容量も大きなものになってしまう。

【０００９】そこで、本発明は、このような従来の問題を解決することを課題としており、暗号化データを生成するときと同一の処理で、その暗号化データを復号化することによって、暗号化／復号化ソフトを開発するために要する費用や時間、または手間などを大幅に削減するとともに、コンパクトなサイズの暗号化／復号化ソフト

を開発することのできるデータ変換装置を提供することを目的としている。

【００１０】

【課題を解決するための手段】上記目的を達成するために、本発明に係る請求項１記載のデータ変換装置は、コンピュータの記憶手段に格納されているデータを、暗号化および復号化するデータ変換装置において、データの所定領域を所定長のエリアが複数個構成されるように分割するデータ分割手段と、特定の組み合わせで対にした前記エリア同士を交換するエリア交換手段と、を備えることを特徴としている。

【００１１】このような構成であれば、平文データを暗号化するときには、暗号化しようとする平文データは、データ分割手段で、所定長のエリアに分割される。そうして、分割された各エリアは、エリア交換手段で、特定の組み合わせで他のエリアと対にされ、それらエリア同士が交換される。したがって、平文データは、分割したエリアの配置が拡散されるので、解読困難な暗号化データに暗号化される。

【００１２】なお、このとき、エリアの長さは、エリアが複数個構成されるように、平文データの長さに応じて決定してもよいし、また逆に、エリアの長さをあらかじめ決定しておき、平文データにダミーデータを付加することによって、エリアが複数個構成されるように調整してもよい。

【００１３】一方、暗号化データを復号化するときには、暗号化データは、データ分割手段で、前記所定長のエリアに分割される。そうして、各エリアは、エリア交換手段で、暗号化したときと同一の組み合わせで他のエリアと対にされ、それらエリア同士が交換される。したがって、暗号化データは、エリアの配置が初期の状態に戻されるため、解読可能な元の平文データに復号化される。

【００１４】なお、ここで、平文データまたは暗号化データは、部分的に暗号化または復号化してもよく、そのような場合には、平文データのうち暗号化しようとする領域を、前記所定長のエリアが複数個構成されるように分割する。ただし、暗号化したときの暗号化領域と、復号化するときの復号化領域とを一致させなければならない。

【００１５】端的にいえば、暗号化データを生成するときと同一の処理で、その暗号化データを復号化するには、平文データを暗号化データに変換する写像関数と、暗号化データを平文データに変換する写像関数とが逆関数の関係にある必要がある。したがって、一のエリアを任意の位置に移動させた場合には、移動先にある他のエリアを、その一のエリアが配置されていた位置に移動することが条件となる。この条件を満たすには、各エリアを対にして交換すればよい。

【００１６】これには、例えば、先頭と末尾とから計数して同一番目に属するエリアを対にし、それらエリア同士を交換するような場合が挙げられる。そうすると、先頭にあるエリアほど末尾に移動させられるので、結果として、変換されたエリアの配置は、元のエリアの配置と逆順となる。

【００１７】また、本発明に係る請求項２記載のデータ変換装置は、請求項１記載のデータ変換装置において、前記データ分割手段は、前記所定領域を前記エリアが偶数個構成されるように分割することを特徴としている。

【００１８】このような構成であれば、平文データまたは暗号化データは、データ分割手段で、エリアが偶数個構成されるように分割される。したがって、分割された各エリアは、必ず他のエリアと対にされて交換される。

【００１９】さらに、本発明に係る請求項３記載のデータ変換装置は、請求項２記載のデータ変換装置において、前記エリア交換手段は、前記すべてのエリアを必ず一度だけ交換する単位交換処理を、少なくとも１回実行することを特徴としている。

【００２０】このような構成であれば、各エリアは、１回の単位交換処理において、対となる他のエリアと必ず１度だけ交換される。そうして、この単位交換処理が１または複数回実行される。

【００２１】ここで、単位交換処理を複数回実行するときには、各単位交換処理ごとに対にするエリアの組み合わせを異ならせることが望ましい。この場合において、組み合わせを異ならせたとしても、単位交換処理でエリアを交換するようにすれば、最初のエリアの配置から複数回の単位交換処理を経て得られたエリアの配置への変換が上記逆関数の関係を満たしているので、例えば、平文データを、異なる複数の単位交換処理Ａ、Ｂ、Ｃの順序で暗号化したときであっても、その暗号化データは、単位交換処理Ａ、Ｂ、Ｃの順序で元の平文データに復号化することができる。

【００２２】また、単位交換処理を含む上記処理を応用した暗号化／復号化ソフトを開発する際には、エリアの分割個数を大きく設定すればするほど、処理パターンを幅広く選択することができる。このため、これらの処理パターンを適宜に組み合わせ、例えば、データの複数の領域について異なる処理パターンで暗号化するなどすれば、バリエーションに富んだソフトを開発することができる。また逆に、このように多数の処理パターンが存在することに着目して、あらかじめいくつかの処理パターンを登録しておき、それら処理パターンのいずれかを指定するようなものを暗号キー／復号キーとして用いることも考えられる。

【００２３】さらに、本発明に係る請求項４記載のデータ変換装置は、請求項１、２または３記載のデータ変換装置において、前記データ分割手段は、さらに前記エリアを所定長のブロックが複数個構成されるように分割するブロック分割処理を、前記すべてのエリアについて等

しく実行し、前記エリア交換手段は、同一エリア内で特定の組み合わせで対にした前記ブロック同士を交換するブロック交換処理を、前記すべてのエリアについて等しく実行することを特徴としている。

【００２４】このような構成であれば、各エリアは、さらに複数のブロックに分割されるが、すべてのエリアにおいて、各エリアごとに構成されるブロックの個数が同数となるように分割される。そうして、エリア内の各ブロックは、特定の組み合わせで他のブロックと対にされて交換されるが、すべてのエリアにおいて、各ブロックが同一の組み合わせで対にされて交換される。

【００２５】この請求項４記載の発明において、特定の組み合わせとは、請求項１記載の発明における特定の組み合わせと同一の組み合わせであってもよいし、異なる組み合わせであってもよい。

【００２６】さらに、本発明に係る請求項５記載のデータ変換装置は、請求項４記載のデータ変換装置において、前記データ分割手段は、前記エリアを前記ブロックが偶数個構成されるように分割することを特徴としている。

【００２７】このような構成であれば、各エリアは、データ分割手段で、ブロックが偶数個構成されるように分割される。したがって、分割された各ブロックは、必ず他のブロックと対にされて交換される。

【００２８】さらに、本発明に係る請求項６記載のデータ変換装置は、請求項１、２、３、４または５記載のデータ変換装置において、データの前記所定領域を構成するビットを反転するビット反転手段を備えることを特徴としている。

【００２９】このような構成であれば、平文データを暗号化するときには、その平文データは、ビット反転手段で、構成するビットが反転されて解読困難な暗号化データに暗号化されるが、暗号化データを復号化するときには、その暗号化データは、反転されたビットがさらに反転されて元の平文データに復号化される。このとき、構成するすべてのビットを反転する必要はなく、特定のビットのみを反転するようにしてもよい。

【００３０】さらに、本発明に係る請求項７記載のデータ変換装置は、請求項１、２または６記載のデータ変換装置において、前記エリアを対にする組み合わせを特定するための特定キーを入力する特定キー入力手段を備え、前記エリア交換手段は、特定キー入力手段から入力された特定キーに基づいて前記各エリアを対にすることを特徴としている。

【００３１】このような構成であれば、分割された各エリアは、エリア交換手段で、特定キー入力手段から入力された特定キーによって特定される組み合わせに基づいて、他のエリアと対にされ、それらエリア同士が交換される。

【００３２】したがって、暗号化データを生成するときに入力した特定キーと、その暗号化データを復号化しようとするときに入力する特定キーとが一致しなければ、その暗号化データは、元の平文データに復号化されない。

【００３３】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら説明する。図１は、本発明に係るデータ変換装置の第１の実施の形態を示す概略構成図である。図２は、図１におけるコンピュータの構成を示すブロック図である。

【００３４】この第１の実施の形態は、本発明に係るデータ変換装置を、図１に示すように、２台のコンピュータ間で、平文データを暗号化して送受信する場合について適用したものである。

【００３５】このデータ変換装置は、平文データを暗号化して送信するコンピュータ１ａと、受信した暗号化データを復号化するコンピュータ１ｂとで構成されており、コンピュータ１ａとコンピュータ１ｂとは、暗号化データを伝送するためのデータ伝送路２で接続されている。

【００３６】同一機能を有する各コンピュータ１ａ，１ｂは、図２に示すように、演算およびシステム全体を制御する演算処理部３と、データの読み出しおよび書き込みが可能な主記憶部４および補助記憶部５と、外部からデータ入力が可能なヒューマンインターフェースとしてのキーボード６と、キーボード６からデータを入力し、かつ、データ伝送路２を介して他方のコンピュータと暗号化データの入出力を行うインターフェース部７とで構成されており、演算処理部３、主記憶部４、補助記憶部５およびインターフェース部７は、データを伝送するためのバスで相互に接続されている。

【００３７】主記憶部４は、ＲＯＭおよびＲＡＭ等の記憶素子からなり、あらかじめ演算処理部３の制御プログラム等が格納されており、補助記憶部４から読み込んだデータおよび演算処理部３の演算過程で必要な演算結果を格納するように構成されている。

【００３８】補助記憶部５は、ハードディスク等からなり、暗号化しようとする平文データ、または、復号化しようとする暗号化データを格納するように構成されている。演算処理部３は、マイクロプロセスユニットＭＰＵ等からなり、補助記憶部５に格納されている平文データを暗号化し、または、暗号化データを復号化しようとするときには、主記憶部４に格納されている所定のプログラムを起動させ、図３のフローチャートに示す処理を実行するように構成されている。ここで、図３は、平文データを暗号化し、または、暗号化データを復号化するための処理を示すフローチャートである。

【００３９】つまり、平文データを暗号化し、または、暗号化データを復号化しようとするときに、演算処理部３では、次のようにして処理を実行する。まず始めに、

図３に示すように、ステップＳ１に移行して、データを格納するためのバッファＢに補助記憶部５から処理対象となる対象データを読み込み、ステップＳ２に移行して、変数ｎに偶数の値をとるエリア数を、変数ｍに偶数の値をとるブロック数を設定し、ステップＳ３に移行して、バッファＢを変数ｎが示す個数のエリアに分割し、さらに、各エリアを変数ｍが示す個数のブロックに分割する。ここで、変数ｎに設定するエリア数および変数ｍに設定するブロック数は、あらかじめ設定した固定の値を用いるものとする。

【００４０】すなわち、バッファＢに読み込んだ対象データは、エリアが変数ｎが示す個数だけ構成されるように分割され、さらに、各エリアは、ブロックが変数ｍが示す個数だけ構成されるように分割される。このとき、エリアの長さは、対象データの長さを変数ｎが示す値で除した値で決定され、ブロックの長さは、同様に、エリアの長さを変数ｍが示す値で除した値で決定される。

【００４１】なお、以降、対象データの先頭からｊ（１≦ｊ≦ｎ）番目のエリアにおいて、そのエリアの先頭からｋ（１≦ｋ≦ｍ）番目のブロックに格納されているデータを示す場合には、Ｂ（ｊ，ｋ）と、ｊ番目のエリアにおいて、すべてのブロックに格納されているデータを示す場合には、Ｂ（ｊ，＊）と表記する。

【００４２】次いで、ステップＳ４に移行して、処理回数を計数するための変数ｊに“１”を設定し、ステップＳ５に移行して、処理回数を計数するための変数ｋに“１”を設定し、ステップＳ６に移行して、バッファＢ（ｊ，ｋ）とバッファＢ（ｊ，ｍ－ｋ＋１）とに格納されているデータを構成するすべてのビットを反転し、ステップＳ７に移行して、バッファＢ（ｊ，ｋ）に格納されているデータとバッファＢ（ｊ，ｍ－ｋ＋１）に格納されているデータとを交換する。そうすると、バッファＢ（ｊ，ｋ）には、バッファＢ（ｊ，ｍ－ｋ＋１）に格納されていたデータを構成するすべてのビットが反転されたものが格納され、バッファＢ（ｊ，ｍ－ｋ＋１）には、バッファＢ（ｊ，ｋ）に格納されていたデータを構成するすべてのビットが反転されたものが格納される。

【００４３】次いで、ステップＳ８に移行して、変数ｋの値に“１”を加算し、ステップＳ９に移行して、変数ｋの値が変数ｍの半値より大きいか否かを判定し、大きいと判定されたときには、ステップＳ１０に移行するが、大きくないと判定されたときには、ステップＳ６に移行する。

【００４４】すなわち、ステップＳ５からステップＳ９までは、変数ｋの値が“１”ずつ増加していくので、ｊ番目のエリアにおいて、そのエリアの半分の位置を対称にして各ブロックが先頭から順次交換されることになる。

【００４５】ステップＳ１０では、変数ｊの値に“１”を加算し、ステップＳ１１に移行して、変数ｊの値が変数ｎの半値より大きいか否かを判定し、大きいと判定されたときには、ステップＳ１２に移行するが、大きくないと判定されたときには、ステップＳ５に移行する。

【００４６】すなわち、ステップＳ４からステップＳ１１までは、変数ｊの値が“１”ずつ増加していくので、すべてのエリアについて、ステップＳ５からステップＳ９までの処理が実行されることになる。

【００４７】ステップＳ１２では、変数ｊに“１”を設定し、ステップＳ１３に移行して、バッファＢ（ｊ，＊）に格納されているデータとＢ（ｎ－ｊ＋１，＊）に格納されているデータとを交換し、ステップＳ１４に移行して、変数ｊの値に“１”を加算し、ステップＳ１５に移行して、変数ｊの値が変数ｎの半値より大きいか否かを判定し、大きいと判定されたときには、ステップＳ１６に移行するが、大きくないと判定されたときには、ステップＳ１３に移行する。

【００４８】すなわち、ステップＳ１２からステップＳ１５までは、変数ｊの値が“１”ずつ増加していくので、対象データの半分の位置を対称にして各エリアが先頭から順次交換されることになる。

【００４９】そうして、ステップＳ１６では、このように対象データのエリアの配置を拡散したものを、補助記憶部５の所定領域に格納して、一連の処理を終了する。次に、上記第１の実施の形態の動作を図面を参照しながら説明する。図４は、平文データを暗号化する場合を説明するブロック図である。図５は、暗号化データを復号化する場合を説明するブロック図である。

【００５０】始めに、コンピュータ１ａの補助記憶部５に格納されている平文データを暗号化して、その暗号化データをコンピュータ２ｂに送信する場合について説明する。

【００５１】まず、データを送信しようとする送信者は、ステップＳ１において、送信対象となる平文データをバッファＢに読み込む。そうすると、ステップＳ２からＳ３までを経て、バッファＢに格納された平文データは、図４（ａ）に示すように、エリアが変数ｎが示す個数（例えば、Ｎ個）構成されるように分割され、さらに、各エリアは、ブロックが変数ｍが示す個数（例えば、Ｍ個）構成されるように分割される。このとき、Ｂ（１，＊）には、データD_1が格納されており、Ｂ（ｊ，１～Ｍ）には、データd_1～d_Mが格納され、Ｂ（Ｎ－ｊ＋１，＊）には、データD_{N-j+1}が格納され、Ｂ（Ｎ，＊）には、データD_Nが格納されているものとする。

【００５２】次いで、ステップＳ４からＳ１１までを経て、各エリア内において、その各ブロックに格納されているデータは、構成するすべてのビットが反転されるとともに、そのエリアの半分の位置Ｍ／２を対称にして交換される。例えば、図４（ｂ）に示すように、ｊ番目のエリアであるＢ（ｊ，＊）では、まず、そのエリアの先

頭にあるデータd_1と末尾にあるデータd_Mとが交換され、次に、先頭から2番目にあるデータd_2と末尾から2番目にあるデータd_{M-1}とが交換され、次に、データd_3とデータd_{M-2}とが、データd_4とデータd_{M-3}とが交換されていく。

【0053】したがって、B（1，＊）には、データD_1内のブロックが交換されたデータ／D_1が格納され、B（j，1～M）には、データd_M～d_1が格納され、B（N－j＋1，＊）には、データD_{N-j+1}内のブロックが交換されたデータ／D_{N-j+1}が格納され、B（N，＊）には、データD_N内のブロックが交換されたデータ／D_Nが格納される。なお、ここで、“／”は、エリア内のブロックが交換された状態のデータを示すための表記である。

【0054】次いで、ステップS12からS15までを経て、各エリアに格納されているデータは、平文データの半分の位置N／2を対称にして交換される。例えば、図4（c）に示すように、まず、平文データの先頭にあるデータ／D_1と末尾にあるデータ／D_Nとが交換され、先頭からj番目にあるデータd_M～d_1と末尾からj番目にあるデータ／D_{N-j+1}とが交換されていく。

【0055】したがって、B（1，＊）には、データ／D_Nが格納され、B（j，＊）には、データ／D_{N-j+1}が格納され、B（N－j＋1，1～M）には、データd_M～d_1が格納され、B（N，＊）には、データ／D_1が格納される。

【0056】すなわち、この平文データは、エリアの配置が拡散されるので、解読困難な暗号化データとなり、ステップS16において、補助記憶部5の所定領域に格納される。そうして、送信者は、この暗号化データをデータ伝送路2を介して、コンピュータ1bに送信する。

【0057】次に、コンピュータ1bにおいて、コンピュータ1aから送信された暗号化データを復号化する場合について説明する。まず、データ伝送路2を介して送信された暗号化データは、インターフェース部7で受信され、補助記憶部5の所定領域に格納される。

【0058】次いで、この暗号化データを受信した受信者は、ステップS1において、復号化しようとするその暗号化データをバッファBに読み込む。そうすると、ステップS2からS3までを経て、バッファBに格納された暗号化データは、図5（a）に示すように、平文データを暗号化したときと同様に、エリアがN個構成されるように分割され、さらに、各エリアは、ブロックがM個構成されるように分割される。このとき、平文データを分割したときと同一のエリア長およびブロック長で暗号化データを分割するので、B（1，＊）には、データ／D_Nが格納され、B（j，＊）には、データ／D_{N-j+1}が格納され、B（N－j＋1，1～M）には、データd_M～d_1が格納され、B（N，＊）には、データ／D_1が格納されていることになる。

【0059】次いで、ステップS4からS11までを経て、各エリア内において、その各ブロックに格納されているデータは、構成するすべてのビットが反転されるとともに、そのエリアの半分の位置M／2を対称にして交換される。

【0060】したがって、図5（b）に示すように、B（1，＊）には、データ／D_N内のブロックが交換されたデータD_Nが格納され、B（j，＊）には、データ／D_{N-j+1}内のブロックが交換されたデータD_{N-j+1}が格納され、B（N－j＋1，1～M）には、データd_1～d_Mが格納され、B（N，＊）には、データ／D_1内のブロックが交換されたデータD_1が格納される。

【0061】次いで、ステップS12からS15までを経て、各エリアに格納されているデータは、暗号化データの半分の位置N／2を対称にして交換される。したがって、図5（c）に示すように、B（1，＊）には、データD_1が格納され、B（j，1～M）には、データd_1～d_Mが格納され、B（N－j＋1，＊）には、データD_{N-j+1}が格納され、B（N，＊）には、データD_Nが格納される。

【0062】すなわち、この暗号化データは、拡散されたエリアの配置が初期の状態に戻されるので、解読可能な元の平文データとなり、ステップS16において、補助記憶部5の所定領域に格納される。

【0063】このようにして、各エリアを対にして交換すれば、平文データを暗号化するときと同一の処理で、暗号化データを元の平文データに復号化することができる。このため、暗号化または復号化するためのデータ処理部とをそれぞれ個別に設計する必要がなく、暗号化／復号化ソフトを開発するために要する時間や費用、または手間などを大幅に削減することができる。

【0064】特に、各エリアをさらに複数のブロックに分割すれば、より解読困難な暗号化データを生成することができるだけでなく、各ブロックを対にする組み合わせが増大するから、それらの組み合わせを適宜に選択してバリエーションに富んだ暗号化／復号化ソフトを開発することができる。

【0065】さらに、対象データを各エリアが偶数個構成されるように分割すれば、各エリアは、必ず他のエリアと対にされて交換されるから、すべてのエリアの配置をもれなく拡散することができる。なお、エリアをブロックに分割する場合についても同様のことがいえる。

【0066】さらに、各エリア同士を交換する際に、そのエリアに格納されているデータを構成するビットを反転させれば、より解読困難な暗号化データを生成することができる。特に、上記処理は、分割したエリアの配置を拡散することを特徴としているため、平文データが文書データである場合に、分割するエリアの長さを大きく設定してしまうと、第三者がその生成された暗号化データを一瞥することによって、暗号化データの拡散規則が

解読される可能性があるが、このように、構成するすべてのビットを反転しておけば、その拡散規則を解読することが極めて困難となる。

【００６７】次に、第２の実施の形態を説明する。この第２の実施の形態は、本発明に係るデータ変換装置を、分割した各エリアを対にする組み合わせに関する情報を暗号キーおよび復号キーとして用いて、平文データを暗号化し、または、暗号化データを復号化する場合について適用したものである。

【００６８】このデータ変換装置は、上記第１の実施の形態における演算処理部３の構成を変更したものであって、演算処理部３は、補助記憶部５に格納されている平文データを暗号化し、または、暗号化データを復号化しようとするときには、図６のフローチャートに示す処理を実行するように構成されている。ここで、図６は、暗号キーによって平文データを暗号化し、または、復号キーによって暗号化データを復号化するための処理を示すフローチャートである。

【００６９】つまり、平文データを暗号化し、または、暗号化データを復号化しようとするときに、演算処理部３では、次のようにして処理を実行する。まず始めに、図６に示すように、ステップＳ２１からＳ２３までを経て、バッファＢに補助記憶部５から対象データを読み込み、変数ｎに偶数の値をとるエリア数を設定し、バッファＢを変数ｎが示す個数のエリアに分割する。ここで、変数ｎに設定するエリア数は、あらかじめ設定した固定の値を用いるものとする。なお、以降、対象データの先頭からｊ（１≦ｊ≦ｎ）番目のエリアに格納されているデータを示す場合には、Ｂ（ｊ）と表記する。

【００７０】次いで、ステップＳ２４に移行して、変数ｘにエリアの配置を拡散するための暗号キーまたは復号キーとなるものをキーボード６から入力する。つまり、対象データをエリアが２Ｎ個構成されるように分割した場合、各エリアを対にする組み合わせの総数は、下式１の右辺に示すだけ存在することから、変数ｘには、これら組み合わせの一を特定する値を設定するようにする。すなわち、変数ｘには、下式１の条件を満たすような自然数を設定する。

【００７１】

$$0 \leqq x < \prod_{i=1}^{N} (2N-2i+1) \qquad (式1)$$

次いで、ステップＳ２５に移行して、処理回数を計数するための変数ｉに“１”を、対にするエリアの一方の位置を特定するための変数Ａに“１”を、フラグデータを格納するための変数Ｃ（１～ｎ）に“０”を設定し、ステップＳ２６に移行して、処理回数を計数するための変数ｊおよびｋに“０”を設定し、ステップＳ２７に移行して、変数Ｃ（Ａ＋ｊ＋ｋ）の値が“０”であるか否かを判定し、“０”であると判定されたときには、ステップＳ２８に移行する。

【００７２】ステップＳ２８では、変数ｋの値が“０”であるか否かを判定し、“０”であると判定されたときには、ステップＳ２９に移行して、変数Ａの値に変数ｊの値を加算し、変数ｊの値に“０”を設定し、ステップＳ３０に移行して、変数ｋの値に“１”を加算し、ステップＳ３１に移行して、変数ｋの値が、変数ｘを（ｎ－ｉ）で除して得た余りに“１”を加算した値よりも大きいか否かを判定し、大きいと判定されたときには、ステップＳ３２に移行する。

【００７３】ステップＳ３２では、バッファＢ（Ａ）に格納されているデータとバッファＢ（Ａ＋ｊ＋ｋ－１）に格納されているデータとを交換し、ステップＳ３３に移行して、変数Ｃ（Ａ）とＣ（Ａ＋ｊ＋ｋ－１）とにそれぞれ“１”を設定する。

【００７４】次いで、ステップＳ３４に移行して、変数ｘに、変数ｘの値を（ｎ－ｉ）で除してその値を整数化したものを設定し、ステップＳ３５に移行して、変数ｉの値が変数ｎの値よりも小さいか否かを判定し、小さくないと判定されたときには、ステップＳ３６に移行し、このように対象データのエリアの配置を拡散したものを、補助記憶部５の所定領域に格納して、一連の処理を終了する。

【００７５】一方、ステップＳ２７で、変数Ｃ（Ａ＋ｊ＋ｋ）の値が“０”でないと判定されたときには、ステップＳ３７に移行して、変数ｊの値に“１”を加算し、ステップＳ３１に移行する。

【００７６】また一方、ステップＳ２８で、変数ｋの値が“０”でないと判定されたときには、ステップＳ３０に移行する。また一方、ステップＳ３１で、変数ｋの値が、変数ｘを（ｎ－ｉ）で除して得た余りに“１”を加算した値よりも大きくないと判定されたときには、ステップＳ２７に移行する。

【００７７】また一方、ステップＳ３５で、変数ｉの値が変数ｎの値よりも小さいと判定されたときには、ステップＳ２６に移行する。次に、上記第２の実施の形態の動作を図面を参照しながら説明する。図７は、暗号キーの値に応じて平文データを暗号化する場合を説明するブロック図である。

【００７８】ここでは、平文データを４つのエリアに分割したときに、入力する暗号キーの値に応じて、それらエリアを対にする組み合わせを決定する場合について説明する。なお、ステップＳ２１からＳ２３までを経て、平文データを４つのエリアに分割したときに、Ｂ（１～４）には、それぞれデータd_1～d_4が格納されているものとする。

【００７９】まず、分割するエリア数は４つであるので、上式１の右辺により、各エリアを対にする組み合わせの総数は、“３”と算出される。このとき、暗号キーとしての変数ｘに設定し得る値の範囲は、上式１より“０”～“２”である。

【００８０】そこで、送信者は、暗号キーとしての変数ｘに“０”を入力するものとすると、ステップＳ２５からＳ２９までを経て、変数Ａには、変数Ａの値“１“と変数ｊの値“０”とを加算した値“１”が設定され、ステップＳ３０からＳ３１までを経て、変数ｋの値“１”が“１”（変数ｘの値“０”を“３”で除して得た余り“０”に“１”を加算した値）よりも大きくないので、ステップＳ２７からＳ２８まで、ステップＳ３０からＳ３１までを経て、変数ｋの値“２”が“１”よりも大きくなったときに、ステップＳ３２に処理が移行される。

【００８１】このとき、変数ｊ、ｋ、Ａの値は、それぞれ“０”、“２”、“１”であるので、ステップＳ３２からＳ３４までを経て、Ｂ（１）に格納されているデータd_1とＢ（２）に格納されているデータd_2とが交換され、変数Ｃ（１）とＣ（２）とに“１”が、変数ｘに“０”が設定される。

【００８２】次いで、ステップＳ２６に処理が戻され、変数Ｃ（１）およびＣ（２）の値が“１”であるので、変数ｊの値が“２”となるが、ステップＳ２９において、変数Ａの値“１”に変数ｊの値が“２”が加算されたときに、変数ｊには、“０”が設定され、ステップＳ３２に処理が移行される。

【００８３】このとき、変数ｊ、ｋ、Ａの値は、それぞれ“０”、“２”、“３”であるので、ステップＳ３２からＳ３６までを経て、Ｂ（３）に格納されているデータd_3とＢ（４）に格納されているデータd_4とが交換される。

【００８４】すなわち、図７の上段に示すように、d_1、d_2、d_3、d_4の順序で構成されていた平文データは、d_2、d_1、d_4、d_3の順序で並び換えられた暗号化データとなる。

【００８５】次に、送信者は、暗号キーとしての変数ｘに“１”を入力するものとすると、ステップＳ２７からＳ３１までを３回繰り返したのちに、ステップＳ３２に処理が移行される。このとき、変数ｊ、ｋ、Ａの値は、それぞれ“０”、“３”、“１”であるので、ステップＳ３２からＳ３４までを経て、Ｂ（１）に格納されているデータd_1とＢ（３）に格納されているデータd_3とが交換され、変数Ｃ（１）とＣ（３）とに“１”が、変数ｘに“０”が設定される。

【００８６】次いで、ステップＳ２７からＳ３１までを２回繰り返したのちに、ステップＳ３２に処理が移行される。このとき、変数ｊ、ｋ、Ａの値は、それぞれ“１”、“２”、“２”であるので、ステップＳ３２からＳ３６までを経て、Ｂ（２）に格納されているデータd_2とＢ（４）に格納されているデータd_4とが交換される。すなわち、図７の中段に示すように、d_1、d_2、d_3、d_4の順序で構成されていた平文データは、d_3、d_4、d_1、d_2の順序で並び換えられた暗号化データとなる。

【００８７】次に、送信者は、暗号キーとしての変数ｘに“２”を入力するものとすると、ステップＳ２７からＳ３１までを４回繰り返したのちに、ステップＳ３２に処理が移行される。このとき、変数ｊ、ｋ、Ａの値は、それぞれ“０”、“４”、“１”であるので、ステップＳ３２からＳ３４までを経て、Ｂ（１）に格納されているデータd_1とＢ（４）に格納されているデータd_4とが交換され、変数Ｃ（１）とＣ（４）とに“１”が、変数ｘに“０”が設定される。

【００８８】次いで、ステップＳ２７からＳ３１までを２回繰り返したのちに、ステップＳ３２に処理が移行される。このとき、変数ｊ、ｋ、Ａの値は、それぞれ“０”、“２”、“２”であるので、ステップＳ３２からＳ３６までを経て、Ｂ（２）に格納されているデータd_2とＢ（３）に格納されているデータd_3とが交換される。

【００８９】すなわち、図７の下段に示すように、d_1、d_2、d_3、d_4の順序で構成されていた平文データは、d_4、d_3、d_2、d_1の順序で並び換えられた暗号化データとなる。

【００９０】なお、これらの暗号化データは、暗号化したときに変数ｘに入力した値と同一の値を入力すれば、解読可能な元の平文データに復号化される。このようにして、分割した各エリアを対にする組み合わせに関する情報を定量的にすれば、通常の暗号化技術のように暗号キー／復号キーを用いるようにした場合であっても、平文データを暗号化するときと同一の処理で、暗号化データを元の平文データに復号化することができる。

【００９１】なお、上記第１の実施の形態においては、各エリアをさらに複数のブロックに分割するように構成した場合について説明したが、これに限らず、各エリアを複数のブロックに分割しないように構成してもよい。

【００９２】また、上記第１の実施の形態においては、エリアを交換する際に、そのエリアに格納されているデータを構成するビットを反転させるように構成した場合について説明したが、これに限らず、ビットを反転させないように構成してもよい。

【００９３】さらに、上記第１の実施の形態においては、各エリアおよびブロックをそれぞれ一度だけ交換するように構成した場合について説明したが、これに限らず、すべてのエリアおよびブロックを必ず１度だけ交換するという処理を単位交換処理とし、各単位交換処理ごとに、対にするエリアの組み合わせを異ならせて、これを複数回実行するように構成してもよい。

【００９４】さらに、上記第１の実施の形態において

は、暗号キー／復号キーを用いないで構成した場合について説明したが、これに限らず、例えば、エリアの分割個数Ｎまたはブロックの分割個数Ｍを暗号キーおよび復号キーとして用いるように構成してもよい。

【００９５】さらに、上記第１の実施の形態においては、ブロック同士を交換してから、エリア同士を交換するように構成した場合について説明したが、これに限らず、エリア同士を交換してから、ブロックを交換するように構成してもよい。

【００９６】さらに、上記第１の実施の形態においては、各エリアをさらに複数のブロックに分割した２段階の構成について説明したが、これに限らず、ブロックをさらに複数の微小なブロックに分割する３段階の構成にしたり、多段階の構成にしたりするのであってもよい。

【００９７】さらに、上記第２の実施の形態においては、各エリアをさらに複数のブロックに分割しないように構成した場合について説明したが、これに限らず、各エリアを複数のブロックに分割するように構成してもよい。

【００９８】さらに、上記第２の実施の形態においては、エリアを交換する際に、そのエリアに格納されているデータを構成するビットを反転させないように構成した場合について説明したが、これに限らず、ビットを反転させるように構成してもよい。

【００９９】さらに、上記実施の形態においては、各エリアまたは各ブロックが偶数個構成されるように分割した場合について説明したが、これに限らず、それらが奇数個構成されるように分割してもよい。そうすると、すべてのエリアまたはブロックのうち、一つだけ交換されないエリアまたはブロックが存在してしまうが、対象データを膨大な数のエリアが構成されるように分割し、さらに、そのエリアも膨大な数のブロックが構成されるように分割すれば、一つだけ交換されていないエリアまたはブロックを発見することが極めて困難となるので、特に問題は生じない。

【０１００】さらに、上記実施の形態においては、エリアに格納されているデータを構成するすべてのビットを反転させるように構成した場合について説明したが、これに限らず、あらかじめ設定した特定のビットのみを反転させるように構成してもよい。このようにすれば、例えば、ビットを反転させる位置を特定する情報を暗号キー／復号キーとして用いることもできる。

【０１０１】さらに、上記実施の形態において、演算処理部３で、図３および図６のフローチャートに示す処理を実行するにあたっては、主記憶部４にあらかじめ格納されているプログラムを実行する場合について説明したが、これに限らず、これらの手順を示したプログラムが記録された記録媒体から、そのプログラムを主記憶部４に読み込んで実行するようにしてもよい。ここで、記録媒体とは、ＲＡＭ、ＲＯＭ、ＦＤ、コンパクトディスク、ハードディスクまたは光磁気ディスク等の記録媒体であって、電子的、磁気的、光学的等の記録方法のいかんを問わず、コンピュータで読み取り可能な記録媒体であれば、あらゆる記録媒体を指していうものである。

【０１０２】さらに、上記実施の形態において、図３および図６のフローチャートに示す処理は、ソフトウェアで構成した場合について説明したが、これに代えて、比較回路、演算回路、論理回路等の電子回路を組み合わせるように構成してもよい。

【０１０３】上記実施の形態において、ステップＳ２およびＳ３、または、ステップＳ２２およびＳ２３は、請求項１、２、４または５記載のデータ分割手段に対応し、ステップＳ１３、または、ステップＳ３２は、請求項１または３記載のエリア交換手段に対応し、ステップＳ４、Ｓ７、Ｓ１０およびＳ１１は、請求項３または４記載のエリア交換手段に対応し、上記単位交換処理を複数回実行する処理は、請求項３記載のエリア交換手段に対応している。

【０１０４】また、上記実施の形態において、ステップＳ６は、請求項６記載のビット反転手段に対応し、キーボード６およびステップＳ２４は、請求項７記載の特定キー入力手段に対応し、ステップＳ２５からＳ３５までは、請求項７記載のエリア交換手段に対応している。

【０１０５】

【発明の効果】以上説明したように、本発明に係るデータ変換装置によれば、暗号化データを生成するときと同一の処理で、その暗号化データを復号化することができるから、暗号化／復号化ソフトを開発するために要する時間や費用、または手間などを大幅に削減することができるとともに、コンパクトなサイズの暗号化／復号化ソフトを開発することができるという効果が得られる。

【０１０６】さらに、本発明に係る請求項４記載のデータ変換装置によれば、エリアをさらに細分化することによって、各ブロックを対にする組み合わせが増大するから、それらの組み合わせを適宜に選択してバリエーションに富んだ暗号化／復号化ソフトを開発することができるという効果も得られる。

【０１０７】さらに、本発明に係る請求項２、４、５または６記載のデータ変換装置によれば、より解読困難な暗号化データを生成することができるという効果も得られる。

【０１０８】さらに、本発明に係る請求項２または５記載のデータ変換装置によれば、すべてのエリアまたはブロックの配置をもれなく拡散することができるという効果も得られる。

【０１０９】さらに、本発明に係る請求項７記載のデータ変換装置によれば、通常の暗号化技術のように暗号キー／復号キーを用いるようにした場合であっても、暗号化データを生成するときと同一の処理で、その暗号化データを復号化することができるという効果も得られる。

【図面の簡単な説明】

【図１】第１の実施の形態の構成を示すブロック図である。

【図２】第１の実施の形態におけるコンピュータ１ａ，１ｂの構成を示すブロック図である。

【図３】データを暗号化または復号化するための処理を示すフローチャートである。

【図４】平文データを暗号化する場合を説明するためのブロック図である。

【図５】暗号化データを復号化する場合を説明するためのブロック図である。

【図６】暗号キー／復号キーを用いてデータを暗号化または復号化するための処理を示すフローチャートである。

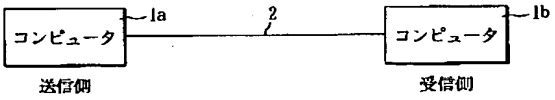
【図７】暗号キーの値に応じて平文データを暗号化する場合を説明するためのブロック図である。

【図８】従来のデータ変換装置におけるデータの処理過程を示すブロック図である。

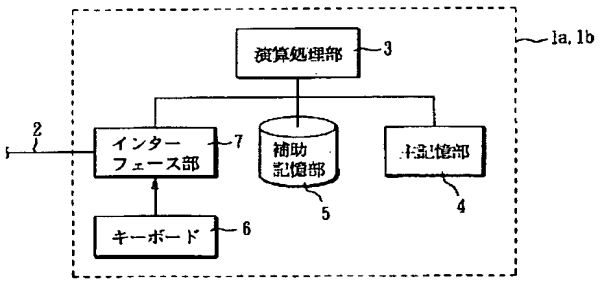
【符号の説明】

１ａ，１ｂ	コンピュータ
2	データ伝送路
3	演算処理部
4	主記憶部
5	補助記憶部
6	インターフェース部
7	キーボード

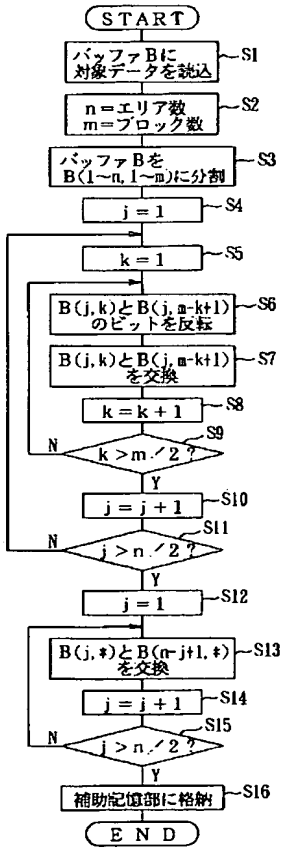
【図１】



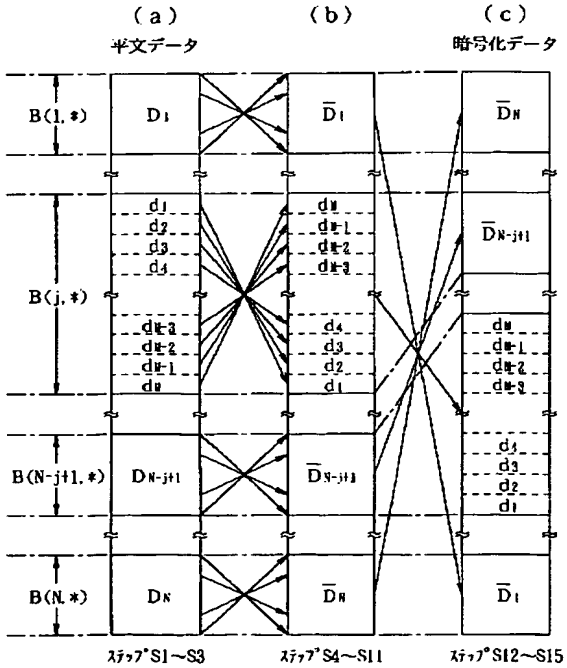
【図２】



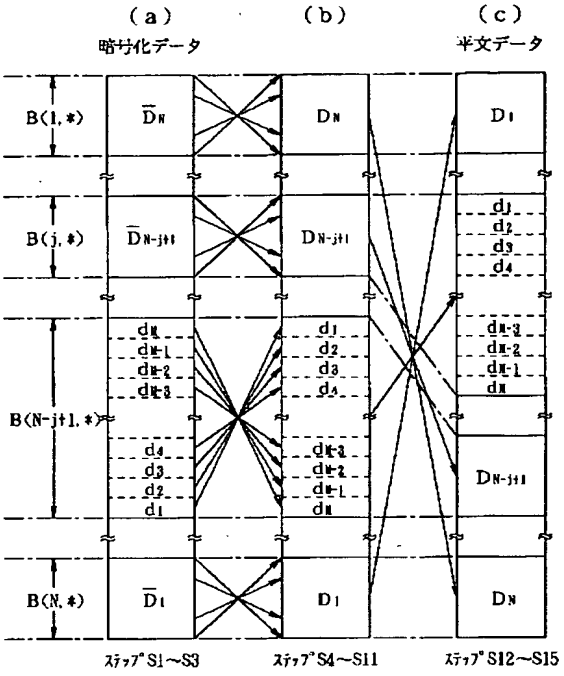
【図３】



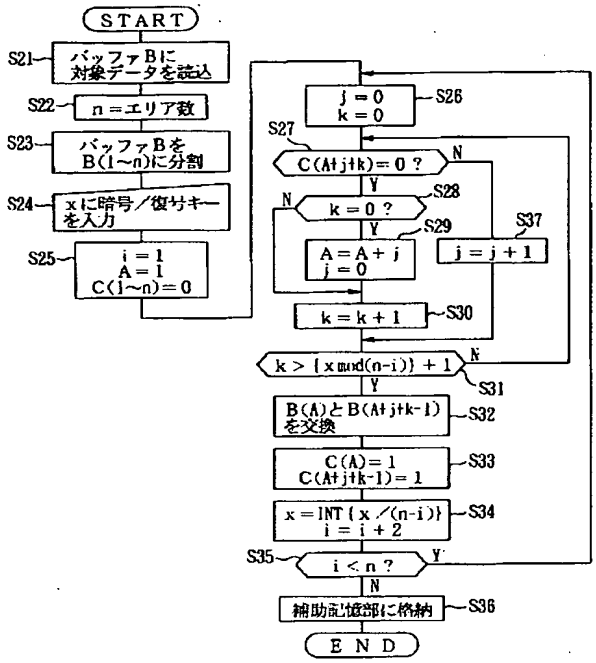
【図４】



【図５】



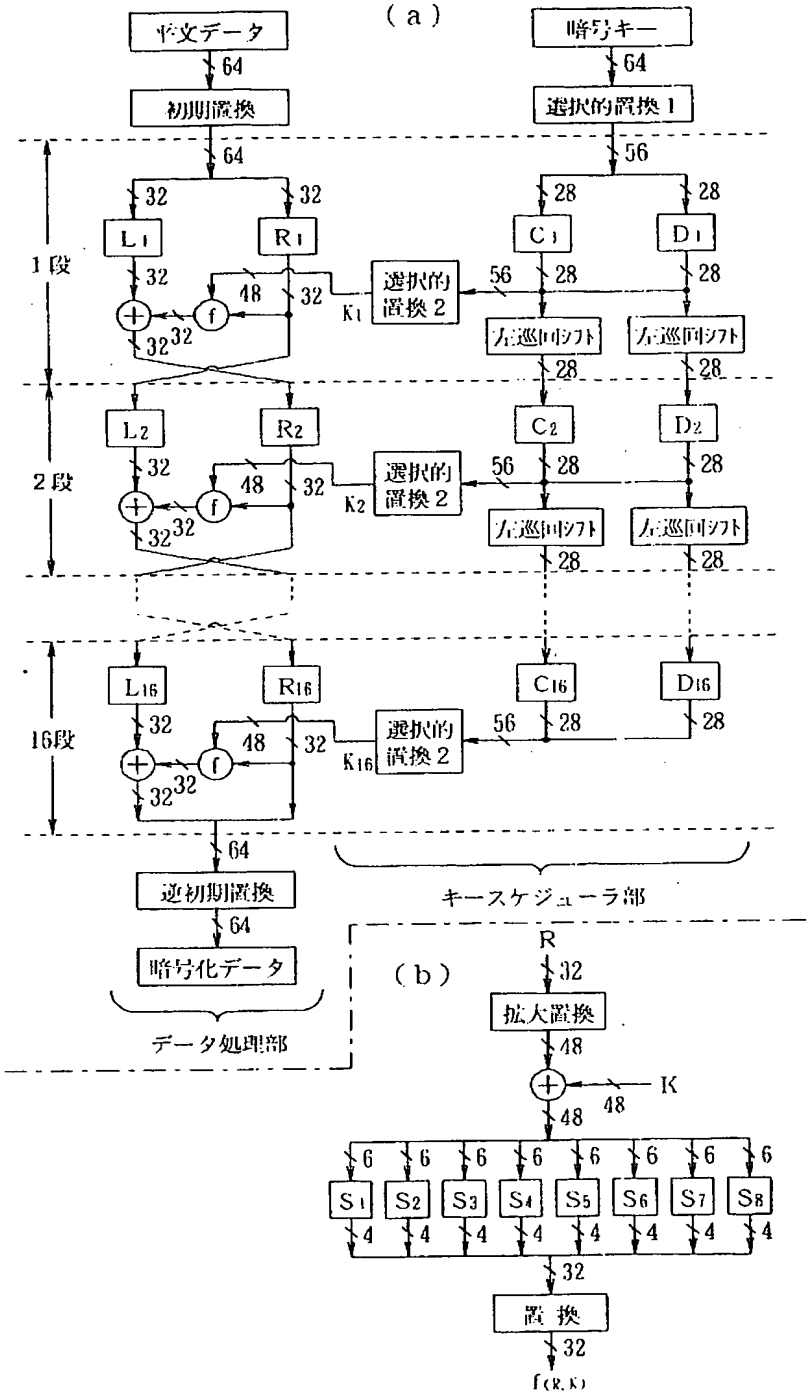
【図６】



【図７】

暗号キーx	平文データ				交換する組み合わせ				暗号化データ			
	B(1)	B(2)	B(3)	B(4)	B(1)	B(2)	B(3)	B(4)	B(1)	B(2)	B(3)	B(4)
0	d1	d2	d3	d4	d1	d2	d3	d4	d2	d1	d4	d3
1	d1	d2	d3	d4	d1	d2	d3	d4	d3	d4	d1	d2
2	d1	d2	d3	d4	d1	d2	d3	d4	d4	d3	d2	d1

【図８】


（ａ）
平文データ
64
初期置換
64
暗号キー
64
選択的置換１
56
32
32
28
28
L1
R1
C1
D1
1段
選択的置換２
K1
左巡回シフト
28
L2
R2
C2
D2
2段
K2
L16
R16
C16
D16
16段
K16
逆初期置換
暗号化データ
データ処理部
キースケジューラ部
（ｂ）
R
拡大置換
48
K
S1
S2
S3
S4
S5
S6
S7
S8
6
4
置換
f(R,K)